AMENDMENTS TO THE CLAIMS

Claims remaining in the application are as follows:

1. (Canceled)

2. (Currently Amended): A method for off-line Personal Identification Number (PIN) verification using a smart card accessed on an off-line terminal, the method ~~according to Claim 1 further~~ comprising:

creating a unique secret key for an enrolled smart card using a card issuer private key;

generating signatures on an entered PIN using the unique key, the signatures being verifiable by the smart card and/or the terminal;

entering an initialization PIN to the smart card at an enrollment system;

generating a reference signature on the initialization PIN using the unique key and the initialization PIN;

storing the reference signature on the smart card; and

discarding the PIN after signature generation.

3. (Original): The method according to Claim 2 further comprising:

communicatively connecting the smart card to an off-line terminal;

receiving a transaction PIN' at the off-line terminal;

generating a candidate signature on the transaction PIN' using the unique key; and

verifying the candidate signature against the reference signature.

4. (Original): The method according to Claim 3 further comprising:

for a verified candidate signature, unlocking the smart card to enable a transaction.

5. (Currently Amended): A method for off-line Personal Identification Number (PIN) verification using a smart card accessed on an off-line terminal, the method ~~according to Claim 1 further~~ comprising:

creating a unique secret key for an enrolled smart card using a card issuer private key;

KOESTNER BERTANI LLP
18662 MACARTHUR BLVD
SUITE 400
IRVINE, CA 92612
TEL (949) 251-0250
FAX (949) 251-0260

generating signatures on an entered PIN using the unique key, the signatures being verifiable by the smart card and/or the terminal;

entering an initialization PIN to the smart card at an enrollment system;

generating the unique secret key based on the private key;

generating at least one signature precursor from the unique secret key;

storing the at least one signature precursor on the smart card; and

discarding the PIN and the unique secret key.

6. (Original): The method according to Claim 5 further comprising:

communicatively connecting the smart card to an off-line terminal;

receiving a transaction PIN' at the off-line terminal;

communicating the transaction PIN' and an off-line terminal-generated random number to the smart card;

generating a signature on the smart card based on the transaction PIN', the at least one signature precursor, and the random number; and

verifying the signature at the off-line terminal.

7. (Canceled)

8. (Currently Amended): A method for off-line Personal Identification Number (PIN) verification using a smart card accessed on an off-line terminal, the method ~~according to Claim 7 further~~ comprising:

using PIN verification to unlock a smart card;

enabling the unlocked smart card to perform a selected function in a financial transaction for a cardholder;

creating a unique secret key for an enrolled smart card using a card issuer private key;

generating signatures on an entered PIN using the unique key, the signatures being verifiable by the smart card and/or the terminal;

computing at an enrollment system a secret key u that is unique to the smart card using an equation of the form:

$$u = I^d (\mathrm{mod}\ N),$$

KOESTNER BERTANI LLP
18662 MACARTHUR BLVD.
SUITE 400
IRVINE, CA 92612
TEL (949) 251-0250
FAX (949) 251-0260

where I is an entity-identifier, d is a private exponent in an RSA system known only to the enrollment system, and N is an RSA system modulus;

computing at the enrollment system a signature precursor A using an equation of the form:

$$A = PIN^{-1} \cdot u (\mathrm{mod}\ N),$$

where PIN is an enrollment Personal Identification Number (PIN);

storing on the smart card the signature precursor A, a public exponent e, the modulus N, and the entity-identifier I;

computing at the smart card a digital signature component t using an equation of the form:

$$t = PIN^{e} (\mathrm{mod}\ N);$$

hashing at the smart card a function Z=h(t, PIN, I) to compute a reference signature of the form:

$$S = u \cdot PIN^{Z} (\mathrm{mod}\ N),$$

where h() is a hashing algorithm;

storing the reference signature S on the smart card; and

erasing from the smart card the enrollment PIN, the secret key u, the digital signature component t, and function Z.

9. (Original): The method according to Claim 8 further comprising:

communicatively connecting a smart card to a transaction terminal;

receiving at the transaction terminal a transaction PIN';

computing at the smart card a transaction secret key u', a transaction digital signature component t', and a transaction function Z', using respective equations of the form:

$$u' = PIN' \cdot A (\mathrm{mod}\ N),$$

$$t' = (PIN')^{e} (\mathrm{mod}\ N), \text{ and}$$

$$Z' = h(t', PIN', I);$$

computing at the smart card a candidate signature S' using an equation of the form:

$$S' = u' \cdot (PIN')^{Z'} (\mathrm{mod}\ N);$$

for S' = S so that PIN' = PIN, verifying PIN'; and

KOESTNER BERTANI LLP
18662 MACARTHUR BLVD.
SUITE 400
IRVINE, CA 92612
TEL (949) 251-0250
FAX (949) 251-0260

unlocking the smart card for a transaction for a verified PIN'.

10. (Currently Amended): The method according to Claim ~~7~~ 8 wherein:

the smart card contains sufficient information to verify an entered PIN prior to proceeding to a transaction; and

the PIN is passed from a transaction terminal to the smart card and remaining verification operations are performed on the smart card.

11. (Currently Amended): A method for off-line Personal Identification Number (PIN) verification using a smart card accessed on an off-line terminal, the method ~~according to Claim 1 further~~ comprising:

creating a unique secret key for an enrolled smart card using a card issuer private key;

generating signatures on an entered PIN using the unique key, the signatures being verifiable by the smart card and/or the terminal; and

enabling a financial terminal to perform a challenge-response protocol to determine whether the smart card and an entered transaction PIN' are valid for a financial transaction to proceed.

12. (Original): The method according to Claim 11 further comprising:

computing at an enrollment system a secret key u that is unique to the smart card using an equation of the form:

$$u = I^d (\mathrm{mod}\ N),$$

where I is an entity-identifier, d is a private exponent in an RSA system known only to the enrollment system, and N is an RSA system modulus;

transferring from the enrollment system to the smart card the secret key u, the identity-identifier I, a public exponent e, and the modulus N, and an entity-selected Personal Identification Number (PIN);

computing at the smart card a signature precursor A using an equation of the form:

$$A = PIN^{-1} \cdot u (\mathrm{mod}\ N); \text{ and}$$

storing on the smart card the signature precursor A, a public exponent e, the modulus N, and the entity-identifier I.

KOESTNER BERTANI LLP
18662 MACARTHUR BLVD
SUITE 400
IRVINE, CA 92612
TEL (949) 251-0250
FAX (949) 251-0260

13. (Currently Amended): The method according to Claim 12 further comprising:

communicatively connecting a smart card to a transaction terminal;

receiving at the transaction terminal ~~a~~ the transaction PIN′;

transferring from the transaction terminal to the smart card a random number r_t generated at the transaction terminal, and an entity-entered PIN′;

waiting at the transaction terminal for a response;

generating at the smart card a random number r_c;

computing at the smart card a transaction digital signature component t, a transaction secret key u′, a hash function Z, and a signature S using respective equations of the form:

$$t = (r_t \cdot r_c \cdot PIN')^c \pmod N,$$

$$u' = PIN' \cdot A \pmod N,$$

$$Z = h(t, PIN', I)$$

$$S = u' \cdot (r_t \cdot r_c \cdot PIN')^Z \pmod N,$$

where h() is a hashing algorithm;

transferring from the smart card to the transaction terminal the signature S and the digital signature component t;

computing at the transaction terminal values $Z = h(t, PIN', I)$; $C = I \cdot t^Z \pmod N$; and $S^c \pmod N$;

determining at the transaction terminal whether $S^c = C \pmod N$, and

if so, verifying the smart card-generated signature S, affirming that PIN′ is equal to PIN.

14. (Currently Amended): The method according to Claim 11 wherein:

the smart card on PIN verification performs operations that verify smart card possession of a secret key created and installed at enrollment of the card, and that verify that ~~a~~ the transaction PIN′ entered by an entity matches the PIN at enrollment;

the verification operations are performed without having the enrollment PIN stored on the smart card; and

KOESTNER BERTANI LLP
18662 MACARTHUR BLVD.
SUITE 400
IRVINE, CA 92612
TEL (949) 251-0250
FAX (949) 251-0260

verification occurs without the smart card revealing the secret key to the transaction terminal.

15. (Currently Amended): The method according to Claim ~~1~~ 8 wherein:
the card issuer private key is an RSA (Rivest, Shamir, and Adelman Public Key Cryptosystem) key.

16. (Original): A data security apparatus comprising:
a smart card capable of off-line Personal Identification Number (PIN) verification comprising:
an interface capable of communicating with an off-line terminal and an enrollment system;
a processor coupled to the interface; and
a memory coupled to the processor and having a computable readable program code embodied therein that executes off-line PIN verification based on creating a unique secret key for an enrolled smart card using a card issuer private key and generating signatures on an entered PIN using the unique key, the signatures being verifiable by the smart card and/or the off-line terminal.

17. (Original): The apparatus according to Claim 16 wherein the memory further comprises:
a computable readable program code capable of causing the processor to receive an initialization PIN from the enrollment system;
a computable readable program code capable of causing the processor to generate a reference signature on the initialization PIN using the unique key;
a computable readable program code capable of causing the processor to store the reference signature on the smart card that is generated from the PIN; and
a computable readable program code capable of causing the processor to discard the PIN without storage after signature generation.

KOESTNER BERTANI LLP
18662 MACARTHUR BLVD.
SUITE 400
IRVINE, CA 92612
TEL (949) 251-0250
FAX (949) 251-0260

18. (Original): The apparatus according to Claim 17 wherein the memory further comprises:

a computable readable program code capable of causing the processor to receive a transaction PIN′ via the off-line terminal;

a computable readable program code capable of causing the processor to generate a candidate signature on the transaction PIN′ using the unique key; and

a computable readable program code capable of causing the processor to verify the candidate signature against the reference signature.

19. (Original): The apparatus according to Claim 18 wherein the memory further comprises:

a computable readable program code capable of causing the processor to enable a transaction for a verified candidate signature.

20. (Original): The apparatus according to Claim 16 wherein the memory further comprises:

a computable readable program code capable of causing the processor to receive an initialization PIN from the enrollment system;

a computable readable program code capable of causing the processor to generate the unique secret key based on the private key and the initialization PIN;

a computable readable program code capable of causing the processor to generate at least one signature precursor from the unique secret key;

a computable readable program code capable of causing the processor to store the at least one signature precursor in the memory; and

a computable readable program code capable of causing the processor to erase the PIN and the unique secret key without storage.

21. (Original): The apparatus according to Claim 20 wherein the memory further comprises:

KOESTNER BERTANI LLP
18662 MACARTHUR BLVD
SUITE 400
IRVINE CA 92612
TEL (949) 251-0250
FAX (949) 251-0260

a computable readable program code capable of causing the processor to receive a transaction PIN′ and a random number from the off-line terminal;

a computable readable program code capable of causing the processor to generate a signature based on the transaction PIN′, the at least one signature precursor, and the random number; and

a computable readable program code capable of causing the processor to send the signature to the off-line terminal for verification.

22. (Original): The apparatus according to Claim 16 wherein the memory further comprises:

a computable readable program code capable of causing the processor to receive from an enrollment system a secret key u that is unique to the smart card and a signature precursor A, the secret key u being defined by an equation of the form:

$$u = I^d (\text{mod } N),$$

where I is an entity-identifier, d is a private exponent in an RSA system known only to the enrollment system, and N is an RSA system modulus,

the signature precursor A being defined by an equation of the form:

$$A = PIN^{-1} \cdot u (\text{mod } N),$$

where PIN is an enrollment Personal Identification Number (PIN);

a computable readable program code capable of causing the processor to store in the memory the signature precursor A, a public exponent e, the modulus N, and the entity-identifier I;

a computable readable program code capable of causing the processor to compute a digital signature component t using an equation of the form:

$$t = PIN^e (\text{mod } N);$$

a computable readable program code capable of causing the processor to hash a function Z=h(t, PIN, I) to compute a reference signature of the form:

$$S = u \cdot PIN^Z (\text{mod } N),$$

where h() is a hashing algorithm;

a computable readable program code capable of causing the processor to store the reference signature S in the memory; and

KOESTNER BERTANI LLP
18662 MACARTHUR BLVD
SUITE 400
IRVINE, CA 92612
TEL (949) 251-0250
FAX (949) 251-0260

a computable readable program code capable of causing the processor to erase the enrollment PIN, the secret key u, the digital signature component t, and function Z from memory.

23. (Original): The apparatus according to Claim 22 wherein the memory further comprises:

a computable readable program code capable of causing the processor to receive from the transaction terminal a transaction PIN′;

a computable readable program code capable of causing the processor to compute a transaction secret key u′, a transaction digital signature component t′, and a transaction function Z′ using respective equations of the form:

$u' = PIN' \cdot A (\bmod N)$,

$t' = (PIN')^e (\bmod N)$, and

$Z' = h(t', PIN', I)$;

a computable readable program code capable of causing the processor to compute a candidate signature S′ using an equation of the form:

$S' = u' \cdot (PIN')^{Z'} (\bmod N)$;

a computable readable program code operative for $S' = S$ so that $PIN' = PIN$ and capable of causing the processor to verify PIN′; and

a computable readable program code capable of causing the processor to enable a transaction for a verified PIN′.

24. (Original): The apparatus according to Claim 16 wherein the memory further comprises:

a computable readable program code capable of causing the processor to receive from an enrollment system a secret key u that is unique to the smart card, the identity-identifier I, a public exponent e, and the modulus N, and an entity-selected Personal Identification Number (PIN), the secret key u being defined by an equation of the form:

$u = I^d (\bmod N)$,

KOESTNER BERTANI LLP
18662 MACARTHUR BLVD
SUITE 400
IRVINE, CA 92612
TEL (949) 251-0250
FAX (949) 251-0260

where I is an entity-identifier, d is a private exponent in an RSA system known only to the enrollment system, and N is an RSA system modulus;

a computable readable program code capable of causing the processor to compute a signature precursor A using an equation of the form:

$$A = PIN^{-1} \cdot u (\mathrm{mod}\ N);$$

a computable readable program code capable of causing the processor to generate a random number r_c; and

a computable readable program code capable of causing the processor to store in the memory the signature precursor A, a public exponent e, the modulus N, and the entity-identifier I.

25. (Original): The apparatus according to Claim 24 wherein the memory further comprises:

a computable readable program code capable of causing the processor to receive from the transaction terminal a random number r_t generated at the transaction terminal, and an entity-entered PIN′, and a random number r_c generated in the smart card;

a computable readable program code capable of causing the processor to compute a transaction digital signature component t, a transaction secret key u′, a hash function Z, and a signature S, using respective equations of the form:

$$t = (r_t \cdot r_c \cdot PIN')^e \ (\mathrm{mod}\ N),$$

$$u' = PIN' \cdot A (\mathrm{mod}\ N),$$

$$Z = h(t, PIN', I)$$

$$S = u' \cdot (r_t \cdot r_c \cdot PIN')^Z (\mathrm{mod}\ N),$$

where h() is a hashing algorithm;

a computable readable program code capable of causing the processor to transfer from the smart card to the transaction terminal the signature S′ and the digital signature component t;

a computable readable program code capable of causing the processor to compute at the transaction terminal values $Z = h(t, PIN', I)$; $C = I \cdot t^Z (\mathrm{mod}\ N)$; and $S^e (\mathrm{mod}\ N)$; and

KOESTNER BERTANI LLP
18662 MACARTHUR BLVD
SUITE 400
IRVINE, CA 92612
TEL (949) 251-0250
FAX (949) 251-0260

a computable readable program code capable of causing the processor to determine at the transaction terminal whether $S^e = C(\text{mod } N)$, and, if so, verify the signature S, affirming that PIN' is equal to PIN.

26. (Original): The apparatus according to Claim 16 wherein:

the card issuer private key is an RSA (Rivest, Shamir, and Adelman Public Key Cryptosystem) key.

27. (Original): A data security apparatus comprising:

an enrollment system capable of usage for off-line Personal Identification Number (PIN) verification using a smart card accessed on an off-line terminal, the enrollment system comprising:

a communication interface capable of communicating with a terminal configured to accept a smart card that executes off-line Personal Identification Number (PIN) verification;

a processor coupled to the communication interface; and

a memory coupled to the processor and having a computable readable program code embodied therein capable of causing the processor to initialize and personalize a smart card for usage in creating a unique secret key for an enrolled smart card using a card issuer private key, and generating signatures on an entered PIN using the unique key, the signatures being verifiable by the smart card and/or the terminal.

28. (Original): The apparatus according to Claim 27 wherein the memory further comprises:

a computable readable program code capable of causing the processor to compute a secret key u that is unique to the smart card using an equation of the form:

$$u = I^d(\text{mod } N),$$

where I is an entity-identifier, d is a private exponent in an RSA system known only to the enrollment system, and N is an RSA system modulus;

a computable readable program code capable of causing the processor to compute a signature precursor A using an equation of the form:

KOESTNER BERTANI LLP
18662 MACARTHUR BLVD.
SUITE 400
IRVINE, CA 92612
TEL (949) 251-0250
FAX (949) 251-0260

$A = PIN^{-1} \cdot u (\mathrm{mod}\ N)$,

where PIN is an enrollment Personal Identification Number (PIN);

transmitting to a smart card for computation and storage the signature precursor A, a public exponent e, the modulus N, and the entity-identifier I, the smart card being capable of computing a digital signature component t using an equation of the form:

$t = PIN^{e} (\mathrm{mod}\ N)$;

hashing at the smart card a function Z=h(t, PIN, I) to compute a reference signature of the form:

$S = u \cdot PIN^{Z} (\mathrm{mod}\ N)$,

where h() is a hashing algorithm, storing the reference signature S; and

erasing the enrollment PIN, the secret key u, the digital signature component t, and function Z.

29. (Original): The apparatus according to Claim 28 wherein the memory further comprises:

a computable readable program code capable of causing the processor to compute a secret key u that is unique to the smart card using an equation of the form:

$u = I^{d} (\mathrm{mod}\ N)$,

where I is an entity-identifier, d is a private exponent in an RSA system known only to the enrollment system, and N is an RSA system modulus;

transferring to the smart card the secret key u, the identity-identifier I, a public exponent e, and the modulus N, and an entity-selected Personal Identification Number (PIN), the smart card being capable of computing at the smart card a signature precursor A using an equation of the form:

$A = PIN^{-1} \cdot u (\mathrm{mod}\ N)$; and

storing the signature precursor A, a public exponent e, the modulus N, and the entity-identifier I.

KOESTNER BERTANI LLP
18662 MACARTHUR BLVD
SUITE 400
IRVINE, CA 92612
TEL (949) 251-0250
FAX (949) 251-0260

30. (Original): A data security apparatus comprising:

30. (Original): A data security apparatus comprising:

an off-line terminal capable of usage for off-line Personal Identification Number (PIN) verification using a smart card, the off-line terminal comprising:

a communication interface capable of accepting and communicating with a smart card that executes off-line Personal Identification Number (PIN) verification;

a processor coupled to the communication interface; and

a memory coupled to the processor and having a computable readable program code embodied therein capable of causing the processor to interact with the smart card to verify an entity-entered PIN using a signature generated on a reference PIN, the signature being generated based on a unique secret key of an enrolled smart card derived from a card issuer private key.

31. (Original): The apparatus according to Claim 30 wherein the memory further comprises:

a computable readable program code capable of causing the processor to communicate with the smart card;

a computable readable program code capable of causing the processor to receive a transaction PIN'; and

a computable readable program code capable of causing the processor to operate in conjunction with the smart card to generate a candidate signature on the transaction PIN' using the unique key, and verify the candidate signature against a reference signature.

32. (Original): The apparatus according to Claim 30 wherein the memory further comprises:

a computable readable program code capable of causing the processor to communicate with the smart card;

a computable readable program code capable of causing the processor to receive a transaction PIN';

KOESTNER BERTANI LLP
18662 MACARTHUR BLVD.
SUITE 400
IRVINE, CA 92612
TEL (949) 251-0250
FAX (949) 251-0260

a computable readable program code capable of causing the processor to generate a random number;

a computable readable program code capable of causing the processor to communicate the transaction PIN′, and the random number to the smart card; and

a computable readable program code capable of causing the processor to operate in conjunction with the smart card to generate a signature based on the transaction PIN′, the at least one signature precursor, and the random number; and verify the signature.

33. (Original): The apparatus according to Claim 30 wherein the memory further comprises:

a computable readable program code capable of causing the processor to communicate with the smart card;

a computable readable program code capable of causing the processor to receive a transaction PIN′; and

a computable readable program code capable of causing the processor to operate in conjunction with the smart card to compute a transaction secret key u′, a transaction digital signature component t′, a transaction function Z′, and a candidate signature S′ using respective equations of the form:

$u' = PIN' \cdot A (\mathrm{mod}\ N)$,

$t' = (PIN')^{e} (\mathrm{mod}\ N)$,

$Z' = h(t', PIN', I)$; and

$S' = u' \cdot (PIN')^{Z'} (\mathrm{mod}\ N)$, and verify whether $S' = S$ so that $PIN' = PIN$, verifying PIN′.

34. (Original): The apparatus according to Claim 30 wherein the memory further comprises:

a computable readable program code capable of causing the processor to communicate with the smart card;

a computable readable program code capable of causing the processor to receive a transaction PIN′;

KOESTNER BERTANI LLP
18662 MACARTHUR BLVD.
SUITE 400
IRVINE, CA 92612
TEL (949) 251-0250
FAX (949) 251-0260

a computable readable program code capable of causing the processor to transfer to the smart card a random number r_t generated at the transaction terminal, and the transaction PIN′;

a computable readable program code capable of causing the processor to wait at the transaction terminal for a response;

a computable readable program code capable of causing the processor to operate in conjunction with the smart card to generate a random number r_c; and

a computable readable program code capable of causing the processor to operate in conjunction with the smart card to compute a transaction digital signature component t, a transaction secret key u′, a hash function Z, and signatures S and C, using respective equations of the form:

$$t = (r_t \cdot r_c \cdot PIN')^e \pmod N),$$

$$u' = PIN' \cdot A(\text{mod } N),$$

$$Z = h(t, PIN', I),$$

$$S = u' \cdot (r_t \cdot r_c \cdot PIN')^Z(\text{mod } N),$$

$$C = I \cdot t^z(\text{mod } N)$$

where h() is a hashing algorithm, and determining at the transaction terminal whether $S^e = C(\text{mod } N)$, and if so, verifying the signature S, affirming that PIN′ is equal to PIN.

35. (Original): The apparatus according to Claim 30 wherein:

the card issuer private key is an RSA (Rivest, Shamir, and Adelman Public Key Cryptosystem) key.

36. (Currently Amended): A transaction system comprising:

a network;

a plurality of servers and/or hosts mutually coupled to the network;

a plurality of terminals capable of communicative coupling to the servers via the network and capable of off-line PIN verification;

a plurality of smart cards capable of enrollment in the transaction system and capable of insertion into the terminals for performing transactions; and

KOESTNER BERTANI LLP
18662 MACARTHUR BLVD.
SUITE 400
IRVINE, CA 92612
TEL (949) 251-0250
FAX (949) 251-0260

a plurality of processors distributed among the smart cards, the servers, and/or the terminals, at least one of the processors being capable of performing a method for off-line Personal Identification Number (PIN) verification comprising:

creating a unique secret key for an enrolled smart card using a card issuer private key; ~~and~~

generating signatures on an entered PIN using the unique key, the signatures being verifiable by the smart card and/or the terminal;

entering an initialization PIN to the smart card at an enrollment system;

generating a reference signature on the initialization PIN using the unique key and the initialization PIN;

storing the reference signature on the smart card; and

discarding the PIN after signature generation.

37. (Currently Amended): A transaction system comprising:

means for verifying a Personal Identification Number (PIN) using a smart card accessed on an off-line terminal;

means for creating a unique secret key for an enrolled smart card using a card issuer private key; ~~and~~

means for generating signatures on an entered PIN using the unique key, the signatures being verifiable by the smart card and/or the terminal;

means for entering an initialization PIN to the smart card at an enrollment system;

means for generating a reference signature on the initialization PIN using the unique key and the initialization PIN;

means for storing the reference signature on the smart card; and

means for discarding the PIN after signature generation.

38. (New): A transaction system comprising:

a network;

a plurality of servers and/or hosts mutually coupled to the network;

a plurality of terminals capable of communicative coupling to the servers via the network and capable of off-line PIN verification;

KOESTNER BERTANI LLP
18662 MACARTHUR BLVD
SUITE 400
IRVINE, CA 92612
TEL (949) 251-0250
FAX (949) 251-0260

a plurality of smart cards capable of enrollment in the transaction system and capable of insertion into the terminals for performing transactions; and

a plurality of processors distributed among the smart cards, the servers, and/or the terminals, at least one of the processors being capable of performing a method for off-line Personal Identification Number (PIN) verification comprising:

creating a unique secret key for an enrolled smart card using a card issuer private key;

generating signatures on an entered PIN using the unique key, the signatures being verifiable by the smart card and/or the terminal;

entering an initialization PIN to the smart card at an enrollment system;

generating the unique secret key based on the private key;

generating at least one signature precursor from the unique secret key;

storing the at least one signature precursor on the smart card; and

discarding the PIN and the unique secret key.

KOESTNER BERTANI LLP
18662 MACARTHUR BLVD
SUITE 400
IRVINE CA 92612
TEL (949) 251-0250
FAX (949) 251-0260